REMARKS

Claim 19 is amended, claims 21-22 are added, and claims 9-11 and 13-22 remain in the application for consideration. In view of the following remarks, Applicant respectfully requests reconsideration and allowance of the subject application.

Examiner Interview

Applicant would like to thank Examiner Gyorfi for discussing this application with Applicant's attorney, Chris Culberson, during a telephonic interview on January 8, 2008.

During this interview, the rejections of the independent claims were discussed, as was the subject matter discussed in the references cited herein. While no specific agreement was reached, Applicant has considered the Examiner's comments and suggestions in crafting this response.

In view of this discussion, Applicant respectfully requests that the Examiner contact Applicant's attorney to discuss this application before issuing any subsequent rejections.

Claim Objections

Claims 21-22 stand objected to for allegedly being improperly labeled. Applicant has relabeled the claims to obviate this objection. Accordingly, Applicant respectfully requests that the objections to claims 21-22 be withdrawn.

§ 103 Rejections

Claims 9-11 and 13-22 stand rejected under 35 U.S.C. § 103(a) for allegedly being obvious over U.S. Patent No. 6,098,079 to Howard in view of the Freenet publication.

The Claims

Claim 9 recites in a distributed file system that stores encrypted files across multiple computers, a method comprising:

- modifying one or more of the encrypted files;
- computing a hash value of each modified encrypted file;
- collecting the hash values into a group;
- computing a hash value of the group; and
- digitally signing the hash value of the group of hash values.

The Office has rejected claim 9 for allegedly being obvious over Howard in view of Freenet. Applicant respectfully disagrees with this rejection and submits that the Office has failed to establish a prima facie case of obviousness with respect to claim 9.

First, the cited combination of references fails to disclose or suggest all of the features recited in claim 9. For example, neither reference discloses or suggests the feature of "computing a hash value of the group [of hash values." In its rejection of this claim, the Office admits that "Howard does not explicitly disclose…that a hash value of the group [of hash values] is computed and digitally

signed." Office Action of October 29, 2007 (hereinafter "Office Action"), at page 3. The Office argues, however, that Freenet discusses this particular feature of claim 9. The Office cites to Freenet as disclosing "an analogous file system (i.e., to Howard) wherein files are hashed and digitally signed…, and that the files on said file system are encrypted." Office Action at page 3. However, this argument still fails to address the feature of "computing a hash value of the group [of hash values]." Simply computing a hash value of a file, as the Office alleges that Freenet discusses, is not that same as or analogous to computing a hash value of a group of hash values. The above-mentioned feature of claim 9 is simply not found in the cited references.

As a further example, the cited combination of references fails to disclose or suggest the feature of digitally signing the hash value of the group of hash values. As discussed above, the cited references fail to disclose or suggest computing a hash value of the group [of hash values]. Thus, since the references do not have a hash value of a group of hash values, the cited references cannot discuss digitally signing a hash value of a group of hash values. This feature is also missing from the cited references.

The Office's prima facie case of obviousness with respect to claim 9 also fails for at least the reason that the Office has failed to provide a sufficient motivation to combine the cited references. The Office states in its rejection that the motivation for combining Howard with Freenet "would be to prevent unauthorized users from tampering with a file to deny other users from accessing

it, and also to provide deniability for legal reasons." Office Action at page 4. However, Freenet refutes this stated motivation. Applicant hereinafter provides an excerpt from Freenet to aid in this discussion:

> For political or legal reasons, it may be desirable for node operators not to explicitly know the contents of their datastores. Therefore, it is recommended that all inserted files be encrypted by their original unhashed descriptive text strings in order to obscure their contents. Of course, this does not secure the file—that would be impossible since a requestor (potentially anyone) must be capable of decrypting the file once retrieved. Rather, the objective is that the node operator can plausibly deny any knowledge of the contents of her datastore, since all she knows a priori is the hashed key and its associated encrypted file. The hash cannot feasibly be reversed to reveal the unhashed description and decrypt the file. With effort, of course, a dictionary attack will reveal which keys are present—as it must in order for requests to work at all.

Freenet at page 7.

Thus, Freenet provides that its encryption scheme "does not secure the file" because "a requestor (**potentially anyone**) must be capable of decrypting the file once retrieved" (emphasis added). Thus, no security is provided by Freenet's encryption scheme and no users are denied access by the scheme. Further, Howard simply discusses "[a] file reconciliation process in a distributed file system uses a set of [journal] or log files to track the history of file modification at each of different sites, or sets of directories, in a computer system." Howard at abstract. Howard displays no need or desire for the "deniability for legal reasons", as alleged by the Office. This appears to be clear case of hindsight reconstruction, as warned against in KSR International v. Teleflex Inc., No. 04-1350 (April 30, 2007). In KSR, the Supreme Court opined that "[a] factfinder should be aware, of

course, of the distortion caused by hindsight bias and must be cautious of arguments reliant upon ex post reasoning." Slip Op. at page 17.

Accordingly, and at least for the reasons discussed above, Applicant submits that the Office has failed to establish a prima facie case of obviousness with respect to claim 9 and claim 9 is allowable.

Claims 10-11 and 13 depend from claim 9 and thus are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 9, are neither disclosed nor suggested in the references of record.

Claim 14 recites one or more computer readable media comprising computer-executable instructions that, when executed, direct a computing device to:

- modify individual files stored in a serverless distributed file system;
- compute a hash value of each modified file;
- collect the hash values into a group; and
- digitally signing the group of hash values.

The Office has rejected claim 14 for allegedly being obvious over Howard in view of Freenet. Applicant respectfully disagrees with this rejection and submits that the Office has failed to establish a prima facie case of obviousness with respect to claim 14.

First, the cited combination references fails to disclose or suggest all of the features recited in claim 14. For example, neither reference discloses or suggests the feature of digitally signing a group of hash values. The Office alleges that

Freenet discloses this particular feature, arguing that "Freenet discloses an analogous serverless distributed file system wherein **files are digitally signed**…." Freenet at page 4 (emphasis added). Whether or not Freenet discusses the subject matter alleged by the Office, this still fails to address the feature of digitally signing **a group of hash values**. This feature is simply missing from the cited references.

Second, the Office has failed to provide a proper motivation to combine the cited references. The Office argues that the motivation for combining Howard and Freenet is "to prevent unauthorized users from tampering with a file to deny other users from accessing it." However, as discussed above, Freenet refutes this motivation in that its encryption scheme provides no file security and does not deny access to files and/or file contents.

Accordingly, and at least for these reasons, the Office has failed to establish a prima facie case of obviousness with respect to claim 14 and claim 14 is allowable.

Claims 15-16 depend from claim 14 and thus are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 14, are neither disclosed nor suggested in the references of record.

Claim 17 recites one or more computer readable media comprising computer-executable instructions that, when executed, direct one or more computing devices to store a data structure comprising:

- representations of modifications made to multiple files stored in a distributed file system such that each said modification has a corresponding said representation;
- a representation of a collection of the representations of the modifications; and
- a digital signature covering at least part of the representations to indicate that the modifications were made by a user with the signature.

The Office has rejected claim 17 for allegedly being obvious over Howard in view of Freenet. Applicant respectfully disagrees with this rejection and submits that the Office has failed to establish a prima facie case of obviousness with respect to claim 17.

First, the cited references fail to disclose or suggest all of the features recited in claim 17. For example, neither reference discloses or suggest the feature of a digital signature covering at least part of the representations [of modifications] to indicate that the modifications were made by a user with the signature. The Office admits that Howard fails to disclose or suggest this particular feature. The Office alleges, however, that Freenet discusses a system in which "a user creates a digital signature covering at least part of the representations of an updated file(s) to indicate that the modifications were made by said user…." Office Action at page 5. Applicant respectfully disagrees that Freenet discusses the subject matter alleged by the Office, and even if it did, this still fails to address the above-mentioned feature.

Freenet discusses a public-private key pair that can be used to determine if a file's contents have been tampered with. Freenet at page 10. However, this fails

to address the feature of a digital signature covering at least part of the representations, the representations being representations of modifications made to **multiple files**. Further, Freenet fails to make any mention of a digital signature **to indicate that modifications were made by a user with the signature**. The public-private key combination of Freenet can be use to distinguish between old and new versions of a file, but Freenet makes no mention of the above-mentioned feature, particularly using a digital signature as discussed in the claim. This feature is simply missing from the cited references.

Second, the Office has failed to provide a proper motivation to combine the cited references. The Office argues that the motivation for combining Howard and Freenet is "to prevent unauthorized users from tampering with a file to deny other users from accessing it." However, as discussed above, Freenet refutes this motivation in that its encryption scheme provides no file security and does not deny access to files and/or file contents.

Accordingly, and at least for these reasons, Applicant submits that the Office has failed to establish a prima facie case of obviousness with respect to claim 17 and claim 17 is allowable.

Claims 18 and 22 depend from claim 17 and thus are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 17, are neither disclosed nor suggested in the references of record.

Claim 19 is amended, and as amended recites a method comprising [added language is indicated in underline]:

- storing representations of modifications made to multiple files stored in a distributed file system such that each said modification has a corresponding said representation;
- storing a representation of a collection of the representations of the modifications; and
- storing a single digital signature covering at least part of the representations to indicate that the modifications were made by a user with the signature, the single digital signature providing file authentication information for each of the multiple files.

The Office has rejected claim 19 for allegedly being obvious over Howard in view of Freenet. While Applicant respectfully disagrees with this rejection, Applicant has nonetheless amended claim 19 to expedite prosecution of this application. Accordingly, Applicant submits that a prima facie case of obviousness with respect to amended claim 19 cannot be established based on this combination of references.

First, the cited references fail to disclose or suggest all of the features recited in claim 19. For example, and as discussed above, neither reference discloses or suggests the feature of a digital signature covering at least part of the representations [of modifications] to indicate that the modifications were made by a user with the signature. This feature is simply missing from the cited references.

As a further example, neither reference discloses or suggests the feature of a single digital signature providing file authentication information for each of the multiple files. The Office cites to Freenet as allegedly discussing a digital signature that "cover[s] at least part of the representations of an updated file(s) to

indicate that the modifications were made by said user." Office Action at page 5. However, Freenet discusses using a public key to "verify that [a] file's contents have not been tampered with." Freenet at page 10, first full paragraph. This fails to address the above-mentioned feature, particular with respect to file authentication information for each of **multiple files**.

Third, the Office has failed to provide a proper motivation to combine the cited references. The Office argues that the motivation for combining Howard and Freenet is "to prevent unauthorized users from tampering with a file to deny other users from accessing it." However, as discussed above, Freenet refutes this motivation in that its encryption scheme provides no file security and does not deny access to files and/or file contents.

Accordingly, and at least for these reasons, Applicant submits that the Office has failed to establish a prima facie case of obviousness with respect to claim 19 and claim 19 is allowable.

Claims 20-21 depend from claim 19 and thus are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 19, are neither disclosed nor suggested in the references of record.

Conclusion

Claims 9-11 and 13-22 are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of the subject application. If any issue remains unresolved that would prevent allowance of this case, the Examiner is requested to urgently contact the undersigned attorney to resolve the issue.

Respectfully Submitted,

Date: January 24, 2008 By: /Christopher J. Culberson
Christopher J. Culberson
Reg. No. 59136
509.755.7266